Practice Guidelines for

Restricted Access Files

Ministry for Children and Families

October 1999

Table of Contents

Introduction

1. Setting restricted access designation on files.....3
2. Accessing information from a restricted access file.....4
3. Monitoring restricted access designation on files.....4
4. Removing restricted access designation on files.....5

Introduction

This document sets out the ministry's practice guidelines for establishing, monitoring and removing Restricted Access files on the SWS system. These guidelines are intended to describe and clarify the expectations and procedures for Ministry for Children and Families (MCF) social workers and team leaders/supervisors regarding restricted access.

Restricted Access files are intended to be used in a limited number of situations where:

- there is a Child Services (CS) file for a child on adoption probation or where the adoption has been completed. This applies where revealing of the identity and location of a child and her/his adoptive family is forbidden under statute;
- personal safety of any person, including a child, could be at risk as a result of the disclosure;
- allowing access to a particular record under the *Child, Family and Community Service Act* may cause unnecessary harm to an individual's reputation in the workplace or community.

Restricted access allows some ministry staff with selected security profiles to query and update file information while providing a means to prevent others from accessing file information. Where restricted access is set on a MCF file, the social worker responsible for the file and her or his supervisor are the only ones who can update information on the file.

All ministry staff and delegated First Nations child welfare directors and social workers involved in child protection will have limited access to MIS information identifying that a record exists and where it is located.

Practice Guidelines

The practice guidelines in this document set out the practice approach for setting, accessing, monitoring and removing restricted access designations from client files to meet all relevant practice standards and facilitate case-specific decision making.

Guiding Principles

These practice guidelines are to be interpreted and administered in accordance with the guiding principles, service delivery principles, and in the best interests of a child, as stated in the *Child, Family and Community Service Act.*

1. Setting restricted access designation on ministry files

Placing a restricted access designation on a file may be considered for the following reasons:

- when a child in care is being placed for adoption, or when the adoption has been completed, restricted access is used to prevent any connection from being made between the Child Service (CS) file and the adopting parents and the community where the child resides.
- where there is concern for the safety and well-being of a client and/or dependents (for example, when a parent is fleeing with her/his children from an abusive or dangerous spouse).
- when knowledge of the contents of a child protection report or/and investigation could be used in the workplace or community to significantly harm the reputation of an individual named in that report or investigation.

Note:
Restricted access cannot be set on a file that has an Alert (ALT) registered on the MIS system by the social worker responsible for the file, or her/his supervisor. There may be situations where a social worker wishes to set restricted access on a file that already has an alert registered on it. In this situation, the social worker contacts the individual who placed the alert on the system and determines whether the reason for placing the alert on the system still exists. If the alert is no longer required, the individual who placed it on the system updates the alert using the "ALT U" screen and then types "N" in the active field. If the alert is still applicable, the team leader/supervisor from each office involved must determine whether the alert or the restricted access request has higher priority.

How restricted access designation is placed on a file?

The social worker makes a request by means of a memo, e-mail or in-person to the team leader/supervisor outlining the reason for the restricted access request. If the team leader/supervisor approves the request then she/he adds restricted access to the file on the MIS. The team leader/supervisor uses the Restricted Access (RAC) screen on the MIS system to set restricted access on a file.

2. Accessing information from a restricted access file

Ministry staff wishing to access information from a restricted access file are to direct their request for file information through their team leader to the team leader or social worker responsible for managing the case file. Information contained in a restricted access file may only be accessed by a child protection worker or her/his supervisor when conducting an assessment of risk to a child or conducting an investigation. Access is limited to child protection workers on a need-to-know basis only. Information requests regarding restricted access files may be made by telephone or electronic means. The supervisor where the file is being managed is to determine if the request for access is appropriate. Information in a restricted access file is to be provided by the social worker or supervisor who manages a restricted access file to a child protection social worker/supervisor conducting a child protection investigation.

All ministry workers and delegated First Nations child welfare directors and social workers involved in child protection will have access to limited MIS information identifying that a record exists and where it is located.

3. Monitoring restricted access designation on files

Social Worker's role

Social workers are responsible for reviewing restricted access files at least every three months to determine whether the restricted access file designation should be removed. The restricted access designation is to be removed when:

- circumstances change where the client and her/his dependent's safety or well-being are no longer an issue.

Team Leader/Supervisor's role

Team leaders/supervisors are responsible for reviewing case specific circumstances with social workers prior to approving and setting a restricted access designation on a ministry file. The team leader/supervisor also determines the appropriateness of a request to access information contained in a restricted access file that she/he is responsible for. Team leaders/supervisors are also responsible for monitoring the appropriateness of maintaining or removing the restricted access file designation on an open or closed file.

How Team Leaders/Supervisors monitor restricted access files

Team leaders/supervisors receive two reports electronically from Systems:

1. Restricted Access Activity
2. Restricted Access Violations.

The Restricted Access Activity report is produced and distributed monthly to team leaders/supervisors. This report identifies all files in the office where restricted access was set or removed within the past month. It is used to monitor restricted access activity.

The Restricted Access Violation report is produced weekly and distributed to team leaders/supervisors. The purpose of this report is to protect clients by listing the files where unauthorised access was attempted. The report provides the team leader/supervisor with a method of monitoring this attempt. Reported violations are to be reviewed and disciplinary action may be considered if an unwarranted violation(s) has occurred.

The team leader/supervisor should meet with social workers responsible for restricted access files at least every three months to determine whether restricted access should continue. Systems Services Branch will produce and distribute a quarterly report that identifies files with a restricted access designation in each office.

4. Removing restricted access designation on files

Who can remove a restricted access designation on a file?

Following a review of the circumstances involved in restricted access designation, the team leader/supervisor may approve a social worker's request to remove restricted access. The team leader/supervisor uses the Restricted Access (RAC) screen on the MIS system to remove restricted access on a file.

A Child Services restricted access file should never have the restricted access designation removed where either the subject of that CS file is being or has been adopted.

Note: After Hours social workers and supervisors have full access to restricted access files.